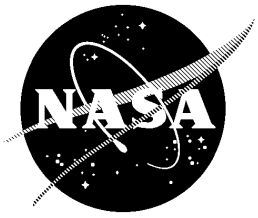
700-DOC-029
(formerly 290-004)

INFORMATION TECHNOLOGY AND COMMUNICATIONS DIRECTORATE

NASA Integrated Services Network (NISN) Internet Protocol Operational Network (IONet) Security Policy

November 2007



National Aeronautics and Space Administration

Goddard Space Flight Center
Greenbelt, Maryland

NASA Integrated Services Network (NISN)
Internet Protocol Operational Network (IONet)
Security Policy

November 2007

Prepared by:

Mary Foote 12/4/07

Mary Foote Date
IONet Security Engineer
Code 730/CSC

Approved by:

Bradford Torain 12/4/07

Bradford Torain Date
NISN Deputy Project Manager
Code 730

Approved by:

M. C. Spinolo 12/4/07

Michael C. Spinolo Date
Alternate IONet Network Security Officer
Code 730

Approved by:

Edwin J. Stevens 1/24/2008

Edwin J. Stevens Date
Chief, Sysyems Management Division
Code 730

Approved by:

Matthew Kirichok 12/4/07

Matthew Kirichok Date
IONet Network Security
Code 730

The contents have been revised and supersede *Internet Protocol Operational Network (IONet) Access Protection Policy and Requirements,* 290-004, dated June 2004, Revision 3.

Goddard Space Flight Center
Greenbelt, Maryland

Preface

The NASA Integrated Services Network (NISN) Internet Protocol Operational Network (IONet) Security Policy document establishes the policy rules and responsibilities for ensuring adequate levels of security confidentiality, availability and integrity for the IONet.

This document is under configuration control. The Information Technology and Communications Directorate (ITCD) is responsible for processing all changes to it. Changes to this document will be issued by Document Change Notice (DCN) or, where applicable, by complete revision. Any questions, recommended changes, or comments concerning this document should be addressed to:

Network Security Officer (NSO)
Code 730
Goddard Space Flight Center
Greenbelt, Maryland 20771

Change Information Page

List of Effective Pages	
Page Number	**Issue**
ii through vi	Original
1-1 through 1-5	Original
2-1 through 2-3	Original
3-1 through 3-6	Original
4-1 through 4-4	Original
5-1	Original
A-1 through A-5	Original
B-1and B-2	Original
C-1 and C2	Original
GL-1 through GL-4	Original
AB-1 and AB-2	Original

Document History			
Document Number	**Status/Issue**	**Publication Date**	**CCR Number**
700-DOC-029	Original	November 2007	730-0487

Contents

Section 1. Introduction

1.1 General

The Internet Protocol (IP) Operational Network (IONet) is a NASA-wide IP network managed by the NASA Integrated Services Network (NISN) Program. The IONet is maintained and operated from the Goddard Space Flight Center (GSFC). The GSFC Information Technology and Communications Directorate (ITCD), Code 700, manages and operates the NISN IONet. The NISN IONet (hereafter referred to as the *IONet*) is an IP network supporting mission-critical spacecraft and science operations and science delivery. IONet's primary customers are NASA space flight programs, which comprise mission control centers; science operations centers; ground terminals for spacecraft tracking networks; and international, contractor, and academia partners who support NASA space flight mission requirements. Facilities are located both inside and outside the United States.

The IONet supports missions on a 24-hour basis with real-time operational data (attitude, command, orbit, ephemeris, telemetry, state vectors). In addition, IONet supports non-real-time data (data products from space experiments, quick-look image data). The IONet is divided into three networks: the Closed IONet, the Restricted IONet, and the Open IONet. The three separate zones of the IONet have separate policies because each network has a different security posture. When referring to all three zones of the network, this document will use the term *IONet*. For other references, the document will specify whether the material pertains specifically to the Open, Restricted, or Closed IONet.

1.2 Acceptable Use

All zones of the IONet perimeter are protected by firewalls. The ITCD at GSFC maintains oversight and control of all the firewalls to control access to or from outside entities. The ITCD at GSFC also monitors the IONet for intrusion detection, suspicious activity, and improper use. The data processed, access allowed, systems connected, dataflows, and network communications on IONet are required to support NASA mission requirements directly. Administrative, general use, or desktop support activities are improper use of the IONet. The detection of non-mission data flows, data processing, and network communications can and will lead to disconnection from the IONet. All network communications on the IONet infrastructure are subject to monitoring, interception, and analysis consistent with Federal and NASA network monitoring policies.

According to the *National Institute of Standards and Technology (NIST) Guide for Mapping Types of Information and Information Systems to Security Categories*, the NIST category for the IONet was determined to be *HIGH* for availability and integrity and *MODERATE* for confidentiality. This designation means that if the IONet information, software applications, network, or computer systems are altered, destroyed, or unavailable, the impact on NASA could be catastrophic. The result may be the loss of major or unique assets, a threat to human life, or prevention of NASA from preparing or training for a critical agency mission. All three IONet

zones handle data that is critical for mission operations and, in the case of the Closed IONet, human spaceflight.

1.3 Purpose

This document fulfills the following functions:

a. States the policy for access to the IONet from any information technology (IT) resource

b. Specifies the security requirements that must be met by customers using the IONet

c. Describes the audit procedures used to evaluate the security controls of IT resources connected to the IONet

d. Describes the procedure for obtaining a connection to the IONet

e. Describes customer IT security documentation that must exist before an IONet connection request will be granted

f. Provides sample Rules of Behavior

g. Outlines the procedures for submission of variance requests for deviations from the policies and requirements levied by this document

h. Outlines the procedures for submission of waiver requests for scanning deviations from NASA policies and requirements

This document specifies requirements for any IT resource that has or is requesting an interface to the IONet. In case of differences between this document and NASA's or any other Federal department's or agency's requirements, the more stringent security requirement takes precedence.

1.4 Applicability

This document is applicable to all NASA field centers, stations, facilities, NASA program offices, NASA contractors, international partner agencies, universities, customers, and commercial ground stations. NISN expects all customers who have IONet access or interface(s) to incorporate the required security safeguards into their contracts, domestic or foreign.

1.5 Applicable Documents

Applicable documents are those that, by virtue of their inclusion in this paragraph, become part of this document and have the same force and authority as if physically reproduced and incorporated as part of this document. Applicable documents are as follows:

a. H.R.2458, E-Government Act of 2002, Title 3, "Federal Information Security Management Act of 2002"

b. NPD 2800.1, Managing Information Technology, March 23, 1998

c. NPD 2810.1, Security of Information Technology, October 1, 1998

d. NPR 2810.1A, Security of Information Technology, May 16, 2006

e. GPG 2810.1, Security of Information Technology Goddard Procedures and Guidelines (GPG), April 16, 2003

f. Office of Management and Budget (OMB) Circular A-130, Appendix III – Security of Federal Automated Information Resources, February 8, 1996

g. SP-800-36, NIST Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004

h. SP-800-47, NIST Security Guide for Interconnecting Information Technology Systems, August 2002

i. SP800-53 Rev.1, NIST Recommended Security Controls for Federal Information Systems, December 2006

j. SP800-30, NIST Risk Management Guide for Information Technology Systems, July 2002

k. SP800-18 Rev.1, NIST Guide for Developing Security Plans for Federal Information Systems, February 2006

l. S800-60, NIST Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004

m. SP-800-34, NIST Contingency Planning Guide for Information Technology Systems, June 2002

n. ITS-SOP 0019.B – Procedure for the FIPS-199 Categorization of Information Systems

o. ITS-SOP 0032 – Master IT Security Plan Template, Requirements, Guidance and Examples

p. ITS-SOP 0016.B - Subordinate IT Security Plan Template, Requirements, Guidance and Examples

q. NPD 1600.2D – NASA Security Policy

r. NPR 1600.1 NASA Security Program Procedural Requirements w/Change 1 (11/08/2005), November 3, 2009

s. FIPS 200 – Minimum Security Requirements for Federal Information and Information Systems

t. NASA SOP, Network Security Vulnerability Scanning, ITS SOP-0021, October 5, 2005

u. NASA memorandum, Office of the Chief Information Officer (NASA HQ), FY 2007 Scanning and Vulnerability Elimination or Mitigation, April 5, 2007

v. NASA memorandum, Office of the Chief Information Officer (NASA HQ), Scanning and Vulnerability Elimination or Mitigation, January 27, 2006

1.6 Authority

The Federal Information Security Management Act (FISMA) was passed by Congress and signed into law by the President as part of the E-Government Act of 2002 (Pub. L. No. 107-347). FISMA goals include development of a comprehensive framework to protect the government's information, operations, and assets. FISMA assigns specific responsibilities to Federal agencies, the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB) to strengthen information system security. In particular, FISMA requires the head of each agency to implement cost-effective policies and procedures to reduce information technology security risks to an acceptable level.

FISMA also requires all Federal IT systems to pass a Certification and Accreditation (C&A) to verify FISMA compliance. NIST has provided guidance for the C&A process, with which all Federal IT Systems must comply. All systems interconnecting with the IONet must satisfy the policies presented in this document, FISMA requirements, and NPR 2810.1A. This document presents additional IT policies specific to the IONet beyond the requirements of NPR 2810.1A.

To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials, Chief Information Officers, and Inspectors General to conduct annual reviews of the agency's information security program and report the results to OMB. Customers and sites connected to the IONet are subject to an audit by NISN's established Mission Operations Security Team (MOST) to ensure that customers comply with Federal and NASA regulations and the access controls in this document. In addition, all Federal programs and their systems that interconnect to IONet must be certified and accredited, as required by FISMA. If the MOST finds the customer out of compliance, any customer is subject to regulation from the Network Security Officer (NSO) and other applicable NISN management. Disciplinary actions may include disconnection from the IONet.

All interconnections with the IONet will be governed by this document and an Interconnect Security Agreement (ISA) that lists specific requirements for the interconnection, authorizing officials, and any additions or exceptions to this control document.

NPR 2810.1A, *Security of Information Technology*, describes the NASA IT Security Program and directs users to the NIST documentation that integrates into and supports the missions of NASA. IONet sensitivity and criticality were determined in accordance with the requirements delineated in NIST SP800-60, *Guide for Mapping Types of Information and Information Systems to Security Categorizations*; ITS-SOP 0019.B; and NPR 2810.1A.

Because the categorization of the IONet is *High*, this document lists security requirements in addition to those listed in the documents in Section 1.4, with which the IT resources interfacing with the IONet must comply.

1.7 Contents and Organization

The remainder of this document is composed of the following sections and appendixes:

a. Section 2. Security Roles and Responsibilities

b. Section 3. IONet Policies and Security Requirements

c. Section 4. MOST-Sponsored Audits

d. Section 5. Connection Request Procedure and Required Security Documentation

e. Appendix A. Sample Rules of Behavior for IT Resources Connected to the IONET

f. Appendix B. IONet Policy Variances

g. Appendix C. IONet Scanning Vulnerability Waivers

h. Glossary

i. Abbreviations and Acronyms

Section 2. Security Roles and Responsibilities

2.1 General

The IONet, like other NASA networks, is designed to provide integrity (ensure that transmitted data is received intact) and availability (network services are performed within an acceptable timeframe). The owner of the node, system, or application is responsible for providing data confidentiality, if needed. As the designer, builder, and manager of the IONet, NISN has the responsibility to secure the IONet infrastructure. In exercising this responsibility, NISN has the right to define requirements that all customers who have access to IONet resources must meet and the right to audit those locations to ensure their compliance.

NISN is responsible for the network's security, the availability of the IONet resources, and data integrity during transmission. NASA Centers and installations play an important part in the overall security operations of the IONet and must comply with the requirements outlined in this document. Users must realize that security is only as strong as its weakest point.

2.2 Responsibilities

NISN is responsible for the following actions:

- Ensure that the security of the IONet is within the bounds of established government, agency, and NISN requirements
- Establish overall IONet Operational Network access policy and requirements
- Establish the rules for connectivity to the IONet; the rules are located in this document
- Provide a real-time network management system to monitor the network continuously
- Perform security audits of customers/sites and system security documentation
- Perform network scanning of equipment connected to the IONet to ensure compliance with the security requirements provided in this document
- Analyze traffic on the IONet through an Intrusion Detection System (IDS)
- Approve and implement the IONet Perimeter Firewall rules; these rules determine what traffic is allowed to flow between the different zones within the IONet and outside entities
- Review and have insight into any approved customer project firewalls connected to the IONet
- Configure the routers connecting the zones of the IONet
- Maintain an active configuration management (CM) system to watch over the IONet's configuration and changes thereto

2.3 Customers

All NASA Centers, international partners, contractors, and commercial ground stations that have connectivity to the IONet are responsible for the following actions:

- Provide security for their IT resources connected to the IONet
- Adhere to all local security requirements and the requirements listed in this document and to appropriate policy and procedural requirements, including but not limited to those imposed by NIST, NPR, and Federal requirements
- Ensure that equipment connected to the IONet has the appropriate physical security controls to prevent unauthorized physical access
- Ensure that no connections to the Open, Restricted, and Closed IONet exist from the same resource, creating possible bypasses around intra-IONet security controls
- Ensure that no connections to the Closed IONet exist from any other network

  Note:

  A firewall between local networks does not provide the required isolation for the Closed IONet. A fundamental security policy of the Closed IONet is that no trust relationship exists between the Closed IONet and the perimeter.

- Report all security incidents to the MOST and to the IONet NSO
- Submit the required documentation (see Section 5.2) with each connection request, when requested by the MOST, or when major changes to connectivity occur

  Note:

  The security evaluation must be completed before a new connection can be installed. Users must allow at least 4 weeks for this evaluation and submit all the required documentation accordingly. In addition, customers must be aware of the NASA requirement to have all documentation approved and signed 30 days prior to the applicable Mission Readiness Review.

- Assist the MOST in performing audits
- Perform or obtain personnel background screening, including fingerprinting, as required by Federal policy
- Establish that each person using the IONet interfaces at his/her job location has a need or requirement for IONet access

2.4 System Administrators and/or System Security Administrators

Each system will have a system administrator (SA) and/or a system security administrator (SSA) (hereinafter referred to simply as *administrator*), who will ensure that the protective security

measures of the system are functional and will maintain its security posture. The administrator is responsible for the following actions:

- Maintain a file of user request forms, signed by a manager, for all accounts entered into the system
- Maintain a file of user-signed Rules of Behavior for all accounts entered into the system
- Correct all known vulnerabilities and report on uncorrected vulnerabilities
- Keep all security patches up to date
- Inform the MOST about administrator or security administration changes and substitutions via e-mail to the NSO within 14 days of the change

2.5 Operators and Users

All personnel with connectivity to the IONet are responsible for the following actions:

- Submit a formal request for a User Identifier (ID) to the local system administrator
- Follow all mandated security procedures
- Follow the requirements outlined in this document, as well as local regulations and NPR 2810.1A
- Report all security incidents (or suspected security incidents) to local authorities and to the Goddard Control Center (GCC) at 301-286-0035
- Sign a statement of responsibility (also known as *Rules of Behavior*), indicating understanding of the requirements for using and safeguarding the information to which access is granted

2.6 IONet MOST

The IONet MOST is responsible for the following actions:

- Review all documentation submitted with connection requests or audits and make recommendations to the IONet NSO
- Perform periodic security audits of all facilities connected to the IONet
- Run network scan and host vulnerability scan programs as requested by the IONet NSO
- Evaluate security technology, as agreed to by the IONet NSO
- Evaluate all variance requests submitted and make recommendations to the IONet NSO for their disposition
- Evaluate all waiver requests submitted and make recommendations to the IONet NSO for their dispositions
- Perform physical site audits as requested and/or approved by the IONet NSO

Section 3. IONet Policies and Security Requirements

The IONet will be used only for NASA mission activities. All workstations, computers, and IT resources connected to the IONet are the ultimate responsibility of the sponsoring program. All resources connected to the IONet must budget for and provide maintenance for the life of the mission. Systems not maintained to current patch levels must be disconnected or waived by the NSO.

3.1 General IONet Security

The IONet infrastructure, including components that interconnect the IONet to its external customer locations, are controlled by NISN personnel. The configuration of these components (routers and conversion devices) is performed at GSFC within the Goddard Communications Control Center (GCC). Customers connecting to the IONet must adhere to the policies and restrictions described in this section. The following policies and restrictions apply to the Open, Restricted, and Closed IONet. Specific restrictions and policies are defined for each zone of the IONet.

3.1.1 IONet Host and Device Registration

All customer systems/hosts that physically connect to the IONet must be registered with the IONet NSO and registered in the internal Mission Network DNS. Unregistered hosts are disallowed and will be considered hostile rogue network hosts and are subject to disconnection without prior customer notice.

Customer managers shall approve and submit to the IONet NSO the name(s) of the operators(s) responsible for registration of the systems. The customers are responsible for keeping the information about the host current with the MOST.

The information to be submitted must include the following details:

- Host name that is unique within the Mission Network
- IP address (will be assigned by the NISN Mission Network IP address manager)
- Split DNS, external or internal DNS only
- SA(s) responsible for the host
- SA(s) phone and e-mail
- Org. Code responsible for system
- Project(s) that this system supports
- Location (i.e., NASA Center, state, street address)
- Building/room number

Submissions are required to be made in Sensitive but Unclassified (SBU) soft-copy form to: Matthew.Kirichok@nasa.gov.

Any systems found to be noncompliant with this policy after 180 days of the effective date of this policy will be disconnected from the IONet until the systems are made compliant.

3.1.2 Domain Name Service (DNS)

The IONet shall be the provider of the DNS service throughout the IONet. The IONet IP DNS manager shall approve the registration and configuration of any DNS server outside the service that the IONet provides. Under ordinary circumstances, customers shall not run any DNS service. For customers behind firewalls and others who are requesting to provide their own DNS service, they are required to submit a variance and register these services with the IONet DNS manager for approval. E-mail the encrypted SBU variance via soft copy to: james.cameron@nasa.gov. Register the services with the IONet DNS manager to: ionet-dns@listserv.gsfc.nasa.gov.

3.1.3 Access to Hosts

Hosts must be pingable throughout the life of the host on the IONet. The ability to ping all hosts aids troubleshooting and scanning hosts (discussed in section 3.1.4). Projects must configure their networks and hosts to allow Inbound "ICMP type 8 echo request" to all hosts connected to the IONet and Outbound "ICMP type 0 echo reply" from all hosts connected to the IONet. If necessary, "ping" rules must be added to the firewall rules to allow this.

3.1.4 Vulnerability Assessments

Vulnerability assessments support agency requirements to protect NASA resources. NASA Headquarters has established the requirement for all NASA organizations to perform vulnerability scanning and to verify that all vulnerabilities are eliminated or mitigated. To support this requirement, the IONet conducts scans: quarterly, when new systems are connected, and on an ad-hoc basis for host vulnerabilities. The IONet keeps a record of vulnerabilities and requires customers either to mitigate vulnerabilities on the devices before the next scan or to request a vulnerability waiver. Failure to correct vulnerabilities is a form of misuse of NASA resources and can result in disconnection from the IONet.

The following are rules pertaining to vulnerability scanning:

a. For connection scans, audit, or certain scheduled ad-hoc scans, projects shall allow the MOST to scan them, even if scanning requires a firewall rule allowing inbound access from the MOST on all ports and protocols. Rules must allow one IONet centralized scanning subnet to obtain access to all hosts on each individual zone. Rules must be maintained for the life of the system as long as it is connected to the IONet.

b. For quarterly scans and other specified ad-hoc scans, projects may keep their personal and/or project firewalls up. If the MOST cannot find any vulnerabilities for quarterly scans, the firewalls have provided a mitigation for these vulnerabilities.

c. The IONet scanning team will perform all scans on the IONet and on the customers connected to the IONet. No one else may perform scans on the IONet.

d. If the SA of the IONet-connected host discovers that the vulnerability reported is a false positive or the vulnerability cannot be eliminated or mitigated, he/she can fill out the IONet scanning waiver form and submit it to the NSO for approval. The NSO will determine whether or not to accept the waiver request. Waivers that are approved are valid for only 1 year, after which the SA has to reapply if he/she still requires the waiver.

e. IONet-connected hosts that are identified with the same vulnerability in three consecutive scanning quarters shall be disconnected from the IONet until the vulnerability is mitigated and the host passes an IONet connection request scan.

3.1.5 National Agency Checks with Inquiries

All personnel with physical or privileged access to IONet-connected resources require a National Agency Check with Inquiries (NAC-I), and those who have privileged or limited privileged access require background screening that includes fingerprinting. A NAC-I "in progress" is not sufficient.

Foreign nationals (including those with a green card) are either non-international or international partners. International partners may not under any circumstances have limited privileged or privileged access to IT resources on the IONet. National partners will abide by the NASA Memorandum of Understanding in place.

3.1.6 IONet Sensitive but Unclassified Information

IONet sensitive information, such as but not limited to IP addresses, vulnerability scan results, firewall rules, passwords, circuit IDs, and special use port numbers, should be handled as Sensitive but Unclassified (SBU), according to NPR 1600.1, Section 5.24.2.1.c. SBU data may only be disclosed to someone who has a valid need to know. If in doubt, the user should ask management. The identity of all personnel to whom SBU data is revealed should be verified. SBU documents and media require a coversheet, NASA form 1686. SBU data must be stored in a secure area under guard or keycard, or have access by lock and key. Transmitting clear text email containing IONet IP addresses, if associated with a customer, is forbidden.

3.2 Encryption on the IONet

The following are rules pertaining to the use of encryption on the IONet:

a. Encrypted communications are permitted only with prior approval by the NSO.

b. Encrypted communications must not traverse the IONet Secure Gateway, which protects the boundary of the Closed IONet.

c. Encrypted connections to IONet-connected resources that cross an IONet firewall are required to be identified by individual IP addresses. Access is required to be restricted to the fewest possible sources. Requests for access from wildcard or subnet sources will be denied. If a system is required to be accessible by a large number of people/systems outside the IONet, such that a wildcard is the only practical way to permit them, system owners/administrators should justify their position in the IONet Firewall Request System.

d. Encrypted tunnels must be configured, where possible, to disallow split tunneling. That is, when connected via an encrypted tunnel to a device connected to the IONet, the client host must not also be able to connect to other networks concurrently.

e. Hosts must employ a host-based firewall configured to limit access to the most restrictive set of allowed connections.

f. IONet hosts providing encrypted communication services should be configured to log all events to a physically separate IONet host.

3.3 IONet Requirements

The following subsections define the requirements for the customers with connection to the Open, the Restricted, and the Closed IONet. The NSO has the authority and jurisdiction over any requirement.

3.3.1 Operations Prohibited on the IONet

The following operations are prohibited on the IONet:

- Remote logins across zones are prohibited. Protocols such as rsh, rlogin, telnet, etc., are prohibited on all devices that support Secure Socket Shell (SSH). SSH v1 is prohibited and must be disabled.
- Dual-homed systems that are connected to two different networks are prohibited. A *dual-homed system* is a system that has multiple network interface cards (NICs) and is connected to two networks at the same time, such as the local center administrative network and the Open IONet. (The IP Transition Network and the Closed IONet are considered the same network: the Closed IONet.)
- Hosts are not permitted to run dynamic routing protocols and/or IP forwarding.
- Project e-mail servers are prohibited.
- Outbound IP traffic from any host on the IONet to an external network using X11 service display is prohibited.
- Network Address Translation (NAT) is prohibited.
- Virtual Private Networks (VPNs) are prohibited between IONet zones.
- Systems should not allow user-initiated actions without authentication.
- Chat, Internet Relay Chat (IRC), and Peer-to-Peer (P2P) messaging/file transfers are all prohibited and must not be installed.
- IONet-connected devices must not have wireless interfaces, make use of wireless communication technologies, or be connected to devices with wireless interfaces.
- Voice over IP (VoIP) is prohibited.
- Dynamic Host Configuration Protocol (DHCP) is prohibited.

- Out-of-band remote access, such as modems or Integrated Services Digital Network (ISDN) lines, is prohibited.
- Mission network hosts are prohibited from leveraging and/or communicating with any Patchlink server other than the NISN Mission/IONet Patchlink system.

3.3.2 Operations Additionally Prohibited on the Closed IONet

In addition to the operations listed in Section 3.3.1, the following operations are prohibited on the Closed IONet:

- Hosts on the Closed IONet cannot connect to any network outside the Closed IONet, except through the Closed IONet firewall.
- All externally sourced connections through the Closed IONet firewall are prohibited.
- Project firewalls are prohibited.

3.3.3 Operations Required on the IONet

The following operations are required on the IONet:

- Adherence to all Agency directives, Standard Operating Procedures, Procedural Requirements, and memoranda is required.
- Restricted physical access is required. Hosts connected to the IONet must be behind locked doors, preferably with at least a key card. If locks are used, there must be a list of personnel with keys, and keyholders must be limited to those with a need to know. Cables must be protected.
- Network services that are not needed must be disabled.
- IONet-connected resources must be maintained with current software revisions—supported by the vendor for security patches—and current patch levels as soon as configuration management policy permits.
- IONet-connected hosts providing communications to non-IONet-connected hosts must be fully patched and are required to install new security patches as soon as configuration management policy permits.
- Network File System (NFS) export files are required to be checked by the MOST. Controlled NFS is allowed within a single subnet within a customer.
- Passwords must be at least eight characters long, must contain a special character, number, and capital and lower case letter. Passwords must be changed at least every 90 days.

3.3.4 Operations Allowed With Limited Use

The use of an IDS outside the customer's subnet is prohibited. Customers may install an IDS within their own systems, but the devices cannot monitor the IONet infrastructure in any way. The use of an IDS requires NSO knowledge.

3.3.5 Variances

Any variations from the policy stated above must be approved by the NSO. Users should follow the approved steps in the variance procedure found in Appendix B.

Section 4. MOST-Sponsored Audits

4.1 MOST Authority and Responsibility

The IONet Most Security Team performs security audits for customers connecting or connected to the IONet to ensure the security of the IONet. The MOST ensures that customers and entities comply with the policy and requirements in this document to protect the integrity of the IONet. Customers must successfully complete Certification and Accreditation (C&A) with NASA as a separate effort. The MOST reviews the C&A risk analysis and summary reports to ensure that the customer connecting to the IONet is not presenting a danger to the IONet. The MOST reports to and takes direction from the IONet NSO.

The IONet NSO has authorized the MOST to view all security features of a system being audited. This authorization includes but is not limited to management controls; access controls; audit trails; password management; monitoring capabilities for IT resources; security-related operational procedures; listings of all authorized customers, entities, and users; and interface descriptions.

The MOST will not attempt to gain physical access to or log onto any system but may perform network scans during the audit process. The MOST may also request a demonstration of or additional information on any system security controls.

The MOST personnel have security clearances at a SECRET level. Upon request, MOST members' security clearances are forwarded to the Customer/Site Security Office before any site visit.

4.2 Reasons for a NISN Audit

Any of the following activities will result in the initiation of an MOST audit:

- Connection request—All requests for new or additional connections to the IONet
- Customer audits—Expansion of a customer's subnet connected to the IONet to support an additional spacecraft or mission
- IONet NSO-requested audits—Any time the IONet NSO requests an audit
- Re-audits—Performed approximately every 3 years or when a major configuration change occurs
- Incident triggered—Any time a customer experiences an IT security incident, such as a compromised system

4.2.1 Connection Request

The Communication Service Manager (CSM) at GSFC informs a customer submitting a Communication Service Request (CSR) or a NISN Service Request (NSR) that a security audit will be performed in parallel with the processing of the connection request. The MOST or the CSM requests that the customer point of contact provide required documentation (refer to Section 5 of this document). The audit then proceeds as described in Section 4.2.4 of this document.

> **Note:**
>
> A customer must be audited before the connection is approved and implemented. A minimum of 4 weeks is required for this process.

4.2.2 Project Audits and IONet NSO-Requested Audits

Audits may be conducted at the request of a customer or the IONet NSO. Upon receiving an audit request, the MOST notifies the customer of the intent to conduct a security audit. The audit then proceeds as described in Section 4.2.4 of this document.

4.2.3 Re-Audits

A complete audit may be performed on all systems that have not been audited in the last 3 years. Re-audits follow the standard audit process described in Section 4.2.4 of this document.

Re-audits concentrate on the following areas:

- Correction of vulnerabilities identified in previous audits
- Significant changes to the system configuration since the previous audit

A *significant change* is any modification that affects the security of a critical system or general support system and requires a new risk analysis. Significant changes include but are not limited to a modification of, deletion of, or addition to a system that might reduce the effectiveness of protective controls or necessitate additional protection.

4.2.4 Audit Process

The audit process is identical for all audits and begins by evaluating the documentation listed in Section 5.2. The customer's designee(s) completes the IONet Access Control Compliance Checklist for the IT resource/network that has an IONet interface. He or she also provides the MOST with all other required documentation for the IT resource/network connection being audited. (Hereafter, the IONet Access Control Compliance Checklist will be referred to as the *checklist*.)

> **Note:**
>
> The checklist, security plans, and risk analysis are considered SBU and must not be sent via clear text email because of the sensitivity of the information. They may be submitted on a compact disc or other such device or through encrypted e-mail.

4.2.5 Step 2 - Documentation Review

The MOST reviews the checklist, the network diagram(s), data flow diagram(s), security plan, Rules of Behavior, and risk analysis required by Section 5 of this document.

The MOST may also request the following types of additional information:

- System-level block diagrams showing the major system components and external interfaces
- Operational procedures, especially if these procedures are part of the system's security
- All variance requests submitted or being submitted and those already approved for the system
- Firewall rules sets

4.2.6 Step 3 - Question Follow-Ups

Documentation and checklist questions can be misinterpreted; information can be incomplete; or the information can generate additional questions. Therefore, a MOST member follow-up on responses is often necessary. A follow-up is conducted through e-mail correspondence. A detailed e-mail is written listing all open issues and questions that must be addressed. This e-mail is the MOST's report back. In addition, telephone conversations and/or face-to-face meetings may occur. The designated person(s) assists the MOST by arranging for follow-up activities with the system managers (SMs) and SAs and any other personnel who helped in completing the checklist. The designated person must ensure the MOST's questions are answered. The MOST updates each checklist based on information gained during the follow-up.

4.2.7 Step 4 - Optional Site Visit

Under certain circumstances, a physical site visit may be required. The MOST determines whether a site visit is necessary, based upon information obtained during documentation review and follow-up activities. The MOST notifies the customer about the intent to conduct a site visit. The designated person makes the necessary arrangements to provide the MOST with any required visitor badges. A knowledgeable SM or SA conducts a system walkthrough with the MOST and should be prepared to perform any requested demonstrations and/or provide additional documentation and/or details supporting the audit.

4.2.8 Step 5 - Audit Findings

During the audit process, the MOST discusses its findings with the designated person(s). The findings are documented in a final audit report. The MOST delivers the audit report to the IONet NSO. The IONet NSO reviews the audit report and takes one of the following actions:

a. Approves a Connection—An e-mail is sent to the designated person, the GCC engineers, and the applicable IONet engineer to allow the connection or continue the connection, based on the security audit findings.

b. Disapproves a Connection—An e-mail is sent to the designated person to explain why the connection has been disallowed. The MOST will work with the customer until all issues are resolved.

c. Directs Disconnection—An e-mail is sent to the responsible Program Manager to identify the issues that have not been resolved. The e-mail will state the deadline by which the issues must be resolved and the date of disconnection if no response is received.

4.2.9 Step 6 - Variance Request

If the MOST identifies anything that does not comply with IONet requirements, the MOST notes the deficiency, brings it to the attention of the designated person, and reports it in the audit report to the IONet NSO. The IONet NSO requires the responsible manager either to correct the deficiency or to submit a variance request. The MOST then verifies that the deficiencies have been corrected. The NSO approves or disapproves the variance request. Variance request forms are found at http://www.nisn.nasa.gov and are discussed further in Appendix B.

Section 5. Connection Request Procedure and Required Security Documentation

5.1 General

The procedure for obtaining a customer connection to the IONet includes the preparation and submission of significant items of documentation and a dialog with the Communications Service Request (CSR) assigned to a customer to ensure completeness.

5.2 Required Security Documentation

The following documentation is required to be submitted before a connection to the IONet is granted:

- Security Plan (see NIST SP-800-18)
- Risk Analysis/Risk Reduction (see NIST SP-800-30)
- Completed IONet Access Control Compliance Checklist (located at http://www.nisn.nasa.gov)
- Detailed network and data flow diagrams
- Authorization to Operate statement, signed by the applicable NASA Headquarters designated person
- Statement that the NPR 2810.1A logon banner is on all NASA-owned or NASA-funded IT systems
- ISA documenting any specific services or exceptions to standard policy
- Individual signed statement of responsibility, often called *Rules of Behavior* (see Appendix A for an example)
- Contingency/Disaster Recovery Plan (see NIST SP-800-34)
- Copy of firewall rules for customer-controlled firewalls

In addition to the above documentation, the MOST will perform a vulnerability scan of all of the customer's systems on the network. In some cases, the team may also perform a physical audit.

> **Note:**
>
> By IONet policy, the documentation listed above must all be approved and signed not less than 30 days before the customer's Mission Readiness Review.

Appendix A. Sample Rules of Behavior for IT Resources Connected to the IONet

These rules apply to all users, including the system administrators, of information technology (IT) resources under the management authority and responsibility of the NISN Mission Network, as identified by the IONet Security Plan. The purpose of these rules is to increase individual awareness and responsibility and to ensure that all users employ IT resources in an efficient, ethical, and lawful manner.

Section 1. Account and Access Control Management

This IT resource account is established only for official use in the conduct of the user's assigned duties. The user understands that all accounts on the IT resources require passwords.

Users must not use the IT resources for fraudulent purposes, harassment, or obscene messages and/or materials. Examples of violations include but are not limited to using these resources to attack other hosts, networks, or users; sending, acquiring, or storing fraudulent, harassing, or obscene messages or messages that contain viruses, worms, trojans, or other damaging programs; using network sniffers/analyzers with authorization; circumventing IONet security procedures; and gaining access to an information technology resource for which authorization has not been given or in excess of the given authorization.

Users shall only use accounts for which they are authorized. Users shall not share accounts and passwords or log in for other users. Users shall not divulge account access procedures to any unauthorized personnel.

Users are responsible for protecting and maintaining, to the best of their ability, any information used or stored in their accounts. Users shall not attempt to access any data or programs contained on systems for which they not authorized or for which they do not have explicit consent of the data/program owner.

Where applicable, all interactive root/administrative access is to be done through first logging in with the user's own account, and then obtaining administrative access by means of su, runas or other such programs, except in emergencies where the user's own account is not available.

If a user leaves the IT resource for a period of time, the user will either log out of the account or immediately lock the screen to prevent unauthorized use of the user's account or the IT resource.

When a user no longer requires access to these IT resources, he or she will notify appropriate responsible parties and make no further attempt to access those resources.

The user will contact his or her SA for additional computing resources or privileges needed to access applications and data. The SA is responsible for granting system privileges.

The SA is required to provide access forms and a copy of the Rules of Behavior form to all new users. All users are required to fill out the access form and have it signed by their manager. They are also required to read the Rules of Behavior form and then sign it. After all of the forms have been signed, they are to be returned to the SA.

Section 2. Authorized Use of Government Equipment

All Government resources (e.g., computer equipment and networks) and electronic communication are for authorized Government business purposes only. While the IT resource is connected to the IONet, all users are required to abide by the most current version of the IONet policy document, 290-004 *Internet Protocol Operational Network (IONet) Access Protection Policy and Requirements* (http://www.nisn.nasa.gov/DocumentPages/Documents.html).

Section 3. Authorized Use of Computers and Computing Resources

Users consent to monitoring and security testing to ensure proper security procedures and appropriate usage are being observed.

Section 4. Dial-In Access

All dial-in access is forbidden, except where approved by the Network Security Officer (NSO).

Section 5. Disclosure Policies

Users should not disclose any information with a Sensitive but Unclassified (SBU) or higher designation to any persons not cleared to receive it or who do not have a need to know without the consent of the NSO, IONet Project Manager, or Operations Manager. People with a need to know include Goddard Comm Control (GCC) Operators, System Administrators, Mission Operations Security Team (MOST) personnel, and Network Engineers. In some cases, users who are calling about a problem may also qualify. For example, users may discuss with such a person their default gateway subnet but should not give them backbone addresses.

Should the Government Official grant his or her permission to disclose Sensitive but Unclassified or above information, the user is expected to follow the given directions on what may be disclosed and to whom.

Section 6. Handling of Sensitive Information

All sensitive information shall be handled in accordance with NPR 1600.1 (http://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=1600&s=1). Sensitive data such as network infrastructure passwords, closed-side host/switch/router configuration information, and closed-side IP addresses shall be protected. Outside physically secure environments, printouts and media that include such data must be carefully controlled and must be destroyed via an approved shredder when no longer in use. Such data should not be stored electronically on open-side or administrative systems except when authorized by the IONet NSO. The data must be then be encrypted and carefully controlled.

Sensitive information (including copyrighted software, personnel information, and proprietary scientific data) shall be removed from hardware devices before they are sent out for repair, excessing, or transfer of ownership. Paper copies of sensitive information are to be shredded, and sensitive information on rewritable media (CDs, DVDs, Tape, USB sticks, or diskettes) is to be erased. CDs, DVDs, tape, USB sticks, or diskettes in the work area with sensitive information are to be stored in locked containers when not in use or before leaving a work area. CDs, DVDs, tape, or diskettes or documents containing sensitive information must be clearly labeled as such.

Section 7. Movement of Computer Equipment

Users are to notify the Property Manager when any government-owned computer equipment is to be excessed, moved or ownership is transferred.

Section 8. Password Management

Passwords are required on all accounts. Passwords must be a minimum length of 8 characters, consisting of at least one character each from at least three of the following sets of characters: uppercase letters, lowercase letters, numbers, and special characters. Users shall not share their password with others. Users are strongly encouraged to use different passwords for each unique machine and for each unique organization (e.g., NASA organizations, university accounts, and private Internet Service Providers).

User passwords must be changed every 90 days, and root/administrative passwords must be changed every 90 days, subject to freezes. Passwords should not be reused for at least 1 year after they are changed.

User passwords and root/administrative passwords are considered extremely sensitive data. They should not be written down and should not be stored electronically, except in encrypted form approved by the NSO. They should not be sent over the network using unencrypted protocols such as telnet, rlogin, rsh, or FTP.

If a user suspects that his or her password has been compromised, the user should immediately change the password and then notify the system administrator or on-duty engineer. If a user suspects a password on a network infrastructure device has been compromised, he or she should immediately inform the On Call Engineer. If a user suspects any other form of security compromise, the user should also immediately inform the GCC and then the SA.

Section 9. Physical Security

The IT resource must be situated in locked rooms/buildings except when such workstations or terminals are located in continuously staffed operational areas.

Section 10. Proper Use of Copyrighted Software

Users must protect all software on the IT resource in accordance with NASA and Federal Government security and control procedures. Users must use licensed software in accordance with the license.

Section 11. Reporting of IT Security Incidents

Users are required to report all observed compromises of IT security (viruses, unauthorized access, theft, inappropriate use, etc.) to the GCC and then their SA. Users must call or visit the GCC and not send clear text e-mail message about the compromise. They can send an encrypted e-mail. If an SA is not available, the user's manager should be informed.

Signature Agreement

This policy remains in effect until superseded. When this policy has been replaced, users who are using the system under current policies no longer have the right to use the systems and must either cease using the systems and inform the SA, or read and sign the new policy.

If you have questions about this policy, please contact your manager, the SA, or the IONet NSO.

Declaration

I HAVE READ AND UNDERSTAND THE RULES OF BEHAVIOR FOR THE USE OF IONET INFORMATION TECHNOLOGY (IT) RESOURCES AND AGREE TO ABIDE BY THEM.

I fully understand my responsibilities as a user of this system/network.

User Name: (please print) _____

User Signature: _____

Organization Code/Contractor Name:

_____

Date: _____

Appendix B. IONet Policy Variances

B.1 Variance Process

If the customer or the MOST uncovers a policy issue that will not be corrected within 3 months, the customer must prepare and submit a Variance Request to the IONet NSO for approval.

The variance request form lists the primary subjects to be addressed: system name, deficiency description, requested duration of the variance, justification, and mitigation. The responsible organization will provide the description of the deficiency and the wording of the variance request necessary to allow an understanding and evaluation of the deficiency by the IONet NSO. A detailed mitigation for the policy variance must be included. The mitigation should be explained in detail to ensure it is fully understood. The IT resource name and deficiency description should be sufficiently unique to allow their use to track the identity of the submission. The responsible organization will submit each variance request on a separate form to assist in the control and processing of requests.

The following Federal requirements cannot be granted a variance:

- Participation in an IT Security Program (OMB Cir A-130)
- Protection of personal information contained in a system of records (PL 93-579, as amended) (Privacy Act)
- Authorization of major applications (OMB Cir A-130)
- Assessment, analysis, and management of risks (OMB Cir A-130)
- Personnel screening for IT access (OMB Cir A-130)
- IT security awareness and training (OMB Cir A-130)
- Response to and reporting of IT security incidents (OMB Cir A-130)
- Mandatory compliance with NIST guidance

B.2 Variance Duration

When a deficiency is recognized, the organization responsible for the IT resource (sponsor) will estimate the time and cost to develop a solution. An estimate of the length of time for which the variance is needed expedites the decision-making process for variance approval and, in addition, establishes a target date for rectification of the variance against policy.

For convenience of reference, variances have been divided into two classes:

- Type 1: Temporary (3 to 6 months)
- Type 2: Long-term (7 to 12 months)

Note:

A variance is valid for up to a maximum of 1 year and must be renewed if the policy condition has not been corrected by the end of 1 year.

B.3 Submission of Variance Requests

All requests for variances of security policy deficiencies found in an IT resource interfacing with IONet shall be forwarded by soft copy or (Public Key Infrastructure) PKI to:

Matthew.Kirichok@nasa.gov

B.4 Variance Approvals

The NSO will designate the MOST team to evaluate all variance request submissions. If the submission lacks adequate information for a comprehensive evaluation, this team will contact the submitting sponsor for additional input. Normally, this approval sequence will be completed within 60 days, unless the variance is of a magnitude that requires consultation with NASA Headquarters.

B.5 Variance Form

The vulnerability variance form can be found at http://www.nisn.nasa.gov. Applicants should ensure that they use the most current form to apply for a variance.

Appendix C. IONet Scanning Vulnerability Waivers

C.1 Waiver Process

If the customer or MOST uncovers a scanning issue that will not be corrected within 3 months, the customer must prepare and submit a waiver request to the IONet NSO for his approval.

The waiver request form lists the primary subjects to be addressed (i.e., system name, deficiency description, requested duration of the waiver, justification, and mitigation). The responsible organization provides the description of the deficiency and the wording of the waiver request necessary to allow an understanding and evaluation of the deficiency by the IONet NSO. A detailed mitigation for the scanning vulnerability must be included. The mitigation should be explained in detail to ensure it is fully understood. The IT resource name and deficiency description should be sufficiently unique to allow their use to track the identity of the submission.

C.2 Waiver Duration

When a deficiency is recognized through the scanning process, the organization responsible for the IT resource (sponsor) will estimate the time and cost to develop a solution. An estimate of the length of time for which the waiver is needed expedites the decision-making process for waiver approval and, in addition, establishes a target date for rectification of the vulnerability.

For convenience of reference, waivers have been divided into two classes:

- Type 1: Temporary (3 to 6 months)
- Type 2: Long-term (7 to 12 months)

> **Note:**
>
> A waiver is valid for up to a maximum of 1 year and must be renewed if the waived condition has not been corrected by the end of 1 year.

C.3 Submission of Waiver Requests

All requests for waivers of security deficiencies found in an IT resource interfacing with IONet shall be forwarded by soft copy or PKI to:

Matthew.Kirichok@nasa.gov

C.4 Waiver Approvals

The NSO will designate the MOST team to evaluate all variance request submissions. If the submission lacks adequate information for a comprehensive evaluation, this team will contact the

submitting sponsor for additional input. Normally, this approval sequence will be completed within 60 days, unless the variance is of a magnitude that requires consultation with NASA Headquarters.

C.5 Waiver Form

The scanning vulnerability waiver form can be found at http://www.nisn.nasa.gov. Applicants should ensure that they use the most current form to apply for a waiver.

Glossary

Access	A specific type of interaction between a subject and an object that results in the flow of information from one to the other.
Access Control	The process of limiting accesses to information or resources of a system to authorized users only.
Audit	The official review, examination, and verification of system records and activities to ensure the adequacy of established IT security controls and procedures and to identify any nonfunctional controls or new vulnerabilities.
Audit Trail	A set of records that collectively provide documentary evidence of processing, used to aid in tracing from the original transactions forward to related records and reports and backward from records and reports to their component source transactions.
Authentication	1) The procedure of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information. 2) The plan designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator.
Availability	The state wherein information, data, and systems are in the place needed by the user, at the proper time, and in the form that the user requests.
Boundary System	A system that is topographically located at the crossroads between an internal local area network (LAN)/wide area network (WAN) and the Internet, usually associated with routing, firewalling, and other security-oriented purposes. A boundary system provides isolation and security services to the systems within a security perimeter.
Confidentiality	The state that exists when data is held in confidence and protected from unauthorized disclosure.
Control	Regulating access to the system.
Dual-Boot System	A computer system in which two operating systems are installed on the same hard drive, allowing either operating system to be loaded and given control.
Dual-Homed	A computer system with two or more network interfaces, each of which is connected to a different network.
DHCP	Dynamic Host Configuration Protocol is an Internet Protocol used for automating the configuration of computers that use TCP/IP. DHCP can be used to assign IP addresses automatically, to deliver TCP/IP stack

	configuration parameters such as the subnet mask and default router, and to provide other configuration information, such as the addresses for printer, time, and news servers.
Firewall	A collection of components used to block or filter transmission of certain classes of traffic; some types of firewalls include stateful inspection packet filtering, circuit gateways, and application gateways.
Identification	The process of providing personal, equipment, or organizational characteristics or codes to gain access to computer resources.
IT	The hardware and software operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information on behalf of the Federal Government to accomplish a Federal function, regardless of the technology involved, whether computers, telecommunications systems, automatic data processing equipment, or other.
IT Resources	Data and information; computers, ancillary equipment, software, firmware, and similar products; facilities that house such resources; services, including support services; and related resources used for the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data. IT resources include telecommunications systems, network systems, and human resources.
Integrity	The state that exists when computerized data is the same as in the source documents or has been correctly computed from source data and has not been exposed to accidental or malicious alteration or destruction.
International Partners	Foreign entities with which business and/or research is conducted; foreign partners may include individuals, small firms, large corporations, and/or foreign governments.
Internet	A collection of two or more disparate networks tied together via a common protocol, more specifically, the global Internet of IP-linked computer networks.
Media	Any and all materials where data and/or information may be stored, including floppy disks, Compact Disc – Read Only Memory (CD-ROMs), hard drives, software manuals, and papers.
Network	A communications medium— and all components attached to that medium—that is responsible for the transfer of information. Such components may include computers, packet switches, telecommunications controllers, key distribution centers, control devices, and other networks.
Object	A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are records, blocks, pages, files, directories, directory trees, and

	programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, and network nodes.
Password	A protected word, phrase, or a string of symbols that is used to authenticate the identity of a user. Knowledge of the password associated with a particular user ID is considered proof of authorization to use the capabilities associated with that user ID.
Physical Security	The application of measures necessary to protect systems and their contents from damage by intruders, fire, accident, and environmental hazards. These measures include electronic security systems, sensors and alarms, lighting, other physical security aids and equipment, and integrated operating procedures.
Process	A program in execution. A process is completely characterized by a single, current execution point (represented by the machine state) and address space.
Risk Analysis	The breakdown and dissection of perceived risks with regard to IT security issues. Analysis of risk involves identifying system vulnerabilities and potential system compromises and indexing the findings in a detailed report.
Routers	Routers connect LANs with common protocols at the network layer and above. Because routers connect at the network layer, they are protocol-sensitive and, thus, can link two TCP/IP, DECnet, or Xerox Network System-based LANs, but not their combinations.
Security Incident	Any circumstance or event that has harmed or has the potential to harm the system in the form of destruction, disclosure, modification of data, and/or denial of service.
Security Measures	The physical, personnel, information, communications, and computer security protective features and procedures applied to systems and facilities to protect classified information and national resources.
Security Plan	A basic overview of the security and privacy requirements of the subject system and the customer's plan for meeting those requirements.
Security Policy	Security policies define access limitations to a LAN, WAN, Internet, Intranet, and Extranet. Security policies must be established before other security provisions can be implemented, such as firewalls and network security standards. Security policies include the following: • Definitions of what is on the trusted and untrusted sides of the network • Policies for protocols to and from the Internet • Access limitations by group and by user to the customer network resources, Intranet, and Extranet and to the Internet

- Access limitations to network resources by external users, both customer employees and others

Significant Change	A modification that affects the security of a critical system or general support system and that requires a new risk analysis. A significant change includes but is not limited to a change in the information category of data processed or stored, replacement of IT equipment with equipment of a different type, new IT equipment to perform new functions, new external interfaces, major changes in connectivity, and relocation of or major changes to the physical environment of an IT resource.
User	Person or process accessing an IT resource either by direct connection (i.e., via terminals) or by indirect connection (i.e., via preparation of input data or receipt of output data that are not reviewed for content or classification by a responsible individual).
Variance	A deviation from IONet policy. A formal grant of relief from meeting a security requirement until a satisfactory solution can be implemented.
Vulnerability	A weakness in system security procedures, system designs, implementation, internal controls, or other system elements that could be exploited to violate system security policy.
Waiver	A scanning vulnerability is encountered on a workstation. Relief provided by the IONet NSO from repairing a detected system or security vulnerability'.

Abbreviations and Acronyms

C&A	Certification and Accreditation
CD	Compact Disc
CM	Configuration Management
COMSEC	Communications Security
CSM	Communication Service Manager
CSR	Communications Service Request
DCN	Document Change Notice
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
E-mail	Electronic Mail
FIPS	Federal Information Processing Standard
FISMA	Federal Information and Security Management Act
FTP	File Transfer Protocol
GCC	Goddard Control Center
GPG	Goddard Procedures and Guidelines
GSFC	Goddard Space Flight Center
ID or IDs	User Identifier(s)
IDS	Intrusion Detection System
IONet	Internet Protocol Operational Network
IP	Internet Protocol
ISA	Interconnect Security Agreement
ISDN	Integrated Services Digital Network
ITCD	Information Technology and Communications Directorate
IT	information technology
ITS	Information Technology Security
LAN or LANs	Local Area Network(s)
MOC	Mission Operations Center

MOST	Mission Operations Security Team
MSFC	Marshall Space Flight Center
NAC	National Agency Check
NAC-I	NAC with Inquiries
NASA	National Aeronautics and Space Administration
NAT	Network Address Translation
NFS	Network File System
NIC	Network Interface Card
NIS	Network Information System
NISN	NASA Integrated Services Network
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
NSM	NISN Service Manager
NSO	Network Security Officer
NSR	NISN Service Request
NTISSP	National Telecommunications and Information Systems Security Policy
OMB	Office of Management and Budget
P2P	Peer-to-Peer
PKI	Public Key Infrastructure
SA	System Administrator
SBU	Sensitive But Unclassified
SCR	Software Change Request
SM	System Manager
SSA	System Security Administrator
SSH	Secure Shell (Secure Socket Shell)
TCP	Transmission Control Protocol
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network